

23. 07. 2003

**PRIORITY DOCUMENT**  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)



**Prioritätsbescheinigung über die Einreichung  
einer Patentanmeldung**

REC'D 12 AUG 2003

WIPO PCT

**Aktenzeichen:**

102 29 704.5

**Anmeldetag:**

02. Juli 2002

**Anmelder/Inhaber:**

Endress + Hauser Process Solutions AG,  
Reinach/CH

**Bezeichnung:**

Verfahren zum Schutz von unerlaubtem Zugriff auf  
ein Feldgerät in der Prozessautomatisierungstechnik

**IPC:**

G 05 B, G 08 C

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 16. Juli 2003  
Deutsches Patent- und Markenamt

Der Präsident  
Im Auftrag

Agurks

## **Verfahren zum Schutz vor unerlaubtem Zugriff auf ein Feldgerät in der Prozessautomatisierungstechnik**

Die Erfindung betrifft ein Verfahren zum Schutz vor unerlaubtem Zugriff auf ein Feldgerät in der Prozessautomatisierungstechnik gemäß dem Oberbegriff des Anspruchs 1.

In der Prozessautomatisierungstechnik werden vielfach Feldgeräte eingesetzt, die in einem industriellen Prozessablauf verschiedene Prozessvariable messen (Sensoren) oder Regelgrößen steuern (Aktoren). Sensoren zur Durchfluss-, Füllstands-, Druck-, Temperaturbestimmung etc. sind allgemein bekannt. Zur Erfassung der entsprechenden Prozessvariablen Massen- oder Volumendurchfluss, Füllhöhe, Druck, Temperatur, etc. sind die Sensoren in unmittelbarer Nähe zu der betreffenden Prozesskomponente angeordnet.

Als Beispiel für Aktoren sind steuerbare Ventile zu nennen, die den Durchfluss einer Flüssigkeit oder eines Gases in einem Rohrleitungsabschnitt regeln.

Die Sensoren liefern Messwerte, die dem aktuellen Wert der erfassten Prozessvariable entsprechen. Diese Messwerte werden an eine Steuereinheit z. B. SPS (Speicherprogrammierbare Steuerung), Warte- oder Prozessleitsystem PLS über einen Datenbus weitergeleitet.

In der Regel erfolgt die Prozesssteuerung von der Steuereinheit, wo die Messwerte verschiedener Feldgeräte ausgewertet werden und aufgrund der Auswertung Steuersignale für die entsprechenden Aktoren erzeugt werden. Neben der reinen Messwertübertragung können Feldgeräte auch zusätzliche Informationen (Diagnose, Status, etc.) an die Steuereinheit übertragen. Die Parametrierung und Konfigurierung der Feldgeräte erfolgt ebenfalls über den Datenbus.

Die Signalübertragung zwischen Feldgerät und Steuereinheit kann in analoger oder digitaler Form erfolgen, bekannte Standards sind HART®, Profibus®, Foundation Fieldbus® oder CAN®-Bus. Vielfach ist der Datenbus mit einem übergeordneten Firmennetzwerk verbunden. Zwischen dem Datenbus (Feldbus) und dem Firmennetzwerk dient ein Controller als Gateway. Über das Firmennetzwerk erfolgt insbesondere die Prozessbeobachtung sowie die Prozessvisualisierung und das Engineering mittels entsprechender Rechneinheiten.

Feldbus und Firmennetzwerk bezeichnet man auch als Prozesskontrollsystem.

Die Sicherheitsanforderungen an Prozesskontrollsysteme werden immer strenger, deshalb sind in vielen Unternehmen Prozesskontrollsysteme von anderen Firmennetzwerken (SAP, Business) streng getrennt. Dadurch sollen unerlaubte Zugriffe auf Feldgeräte vermeiden werden. Momentan konzentrieren sich die Anstrengungen im Hinblick auf Sicherheit bei Prozesskontrollsystemen auf die Netzwerk-Ebene.

Zur Vermeidung von firmenfremden Angriffen werden sogenannte Firewalls eingesetzt. Neben firmenfremden Angriffen sind aber firmeninterne Angriffe ebenso gefährlich. Bei firmeninternen Angriffen können z. B. Parameter in Feldgeräten geändert werden oder die gesamte Kontrollstrategie geändert werden. Dies kann zu erheblichen Produktionsstörungen führen.

Aus diesem Grunde sind Programme, die die Parametrierung, Konfigurierung und eine Veränderung der Kontrollstrategie ermöglichen (SCADA-Systeme oder Configuration Tools) mit einem Passwortschutz ausgestattet. Hierbei ist auch eine Authorisierung der Personen die Änderungen durchführen notwendig.

Z. B. können bei dem Centum CS 1000 Prozesskontrollsystem von Yokogawa kritische Funktionsblöcke, die z.B. in Feldgeräten ablaufen, nur über die Eingabe von zwei Passwörtern verschiedener Personen geändert werden.

Bei der Firma Endress + Hauser gibt es ein Sicherheitsschutz gegen unberechtigtes ändern von Parametern bei Feldgeräten über eine Verriegelung. Die Person, die Änderung vornehmen möchte, muss am Feldgerät einen Code eingeben bevor Änderungen am Feldgerät möglich werden.

Heutige Prozesskontrollsysteme arbeiten häufig auf Ethernet-Basis. Hierbei ist es relativ einfach über eine entsprechende Konfiguriereinheit (Laptop, Handheld) direkt auf die Feldgeräte zuzugreifen und dabei Parameter und Einstellungen an diesen zu ändern. Mit einer derartigen zusätzlichen Konfiguriereinheit ist es ohne weiteres möglich auch die gesamte Kontrollstrategie zu ändern.

Eine Kontrollstrategie kann z. B. mit dem 302 Syscon von der Firma SMAR erzeugt werden und in die Feldgeräte geladen werden.

Aufgabe der Erfindung ist es ein Verfahren zum Schutz vor unerlaubtem Zugriff auf ein Feldgerät anzugeben, das unerlaubte Änderungen an der Konfigurierung von Feldgeräten verhindert und das kostengünstig und einfach durchführbar ist.

Gelöst wird diese Aufgabe durch das in Anspruch 1 angegebene Verfahren.

Wesentliche Idee der Erfindung ist es, im Feldgerät selbst ein Sicherheitsprogramm abzuspeichern, das bei einem Zugriff auf das Feldgerät über den Datenbus eine Berechtigungsprüfung durchführt. Dadurch kann

eine Manipulation am Feldgerät durch Nichtberechtigte in einfacher Weise verhindert werden.

Vorteilhafte Weiterentwicklung der Erfindung sind in den Unteransprüchen angegeben.

Nachfolgend ist die Erfindung anhand eines in der Zeichnung dargestellten Ausführungsbeispiels näher erläutert.

Figur 1 zeigt ein Prozesskontrollsystem das einen Datenbus 5 und ein Firmennetzwerk 15 die über einen Controller 7 (Linking Device) miteinander verbunden sind, umfasst. An den Datenbus 5 ( Feldbus) sind verschiedene Sensoren S1, S2, S3, S4 angeschlossen, die zur Bestimmung der Füllhöhe h einer Flüssigkeit in einem Behälter 1 dienen. Am Behälter 1 ist weiterhin eine Anzeigeeinheit 4 angeordnet. Der Datenbus 5 ist weiterhin mit einer Remote I/O- Einheit 9 verbunden, die den Anschluss verschiedener 4 bis 20 mA Messgeräte erlaubt.

An das Firmennetzwerk 15 sind verschiedene Rechnersysteme 11, 12 angeschlossen, die z. B. eine Prozessvisualisierung ermöglichen oder zum Engineering der Prozessanlage dienen.

In Figur 2 ist ein Funktionsblock dargestellt, der definierte Kommunikationsschnittstellen aufweist.

Moderne Datenbusse erlauben nicht nur die Datenübertragung zwischen einem Sensor und einer übergeordneten Einheit sondern auch die Ausführung standardisierter Anwendungsfunktionen wie sie z. B. durch die Fieldbus Foundation® oder die Profibus Nutzer Organisation PNO ® definiert sind. Funktionsblöcke besitzen eine selbständige Kommunikationsfähigkeit und erlauben im Zusammenspiel mit unterschiedlichen Feldgeräten komplizierte Steuervorgänge auszuführen.

Ein einfacher Funktionsblock ist ein PID-Regler der mit einem Funktionsblock in einem Sensor und einem Aktor kommuniziert. In Fig. 2 ist ein PID-Regler Funktionsblock PID dargestellt, der mit einem Analog Input AI und einem Analog Output AO- Funktionsblock verbunden ist. Die Parameter der Funktionsblöcke werden bei der Konfiguration und Parametrierung der Feldgeräte festgelegt. Sie bestimmen im wesentlichen die Funktionalität des Feldgerätes bzw. der Kontrollstrategie. Da sich bei Funktionsblöcken um standardisierte Anwendungsfunktionen handelt, erlauben sie das Zusammenspiel von verschiedenen Feldgeräten unterschiedlicher Hersteller zur Ausführung aufwendiger Kontrollstrategien.

Mit Hilfe von entsprechenden Tools (z.B. Syscon 302) kann die gesamte Kontrollstrategie bzw. einzelne Parameter von Funktionsblöcken geändert werden. Dies kann bei unberechtigtem Zugriff zu erheblichen Fehlfunktionen im Prozessablauf führen.

Ein wesentlicher Aspekt der Erfindung ist es, im Feldgerät ein Sicherheitsprogramm abzuspeichern, das bei einem Zugriff auf das Feldgerät über den Datenbus eine Berechtigungsprüfung des Zugriffs durchführt. Greift ein Unberechtigter über den Datenbus auf das Feldgerät zu und versucht Parameter von im Feldgerät abgespeicherten Funktionsblöcke zu ändern oder Funktionsblöcke auszutauschen, so wird dies durch die Berechtigungsprüfung verhindert. Nur berechnigte Personen haben Zugriff auf das Feldgerät.

In einfacher Weise ist das Sicherheitsprogramm Teil eines Funktionsblocks. Alternativ kann das Sicherheitsprogramm auch Teil einer im Feldgerät abgespeicherten Firmware sein.

Das Sicherheitsprogramm umfasst z. B. einen Sicherheitsschlüssel der aus einem 128 Bit-Code oder einem längerem Bit-Code besteht. Je mehr Bits der Code aufweist, desto schwieriger ist ein „Knacken“ des Codes.

Der Sicherheitsschlüssel kann bei der Installation des Feldgerätes erzeugt und in diesem abgespeichert werden.

Alternativ ist der Sicherheitsschlüssel bereits im Feldgerät abgespeichert.

Nur mit dem richtigen Sicherheitsschlüssel lassen sich Änderungen an den Einstellungen des Feldgerätes insbesondere an den Funktionsblöcken vornehmen.

Es gibt prinzipiell zwei Möglichkeiten auf das Feldgerät zuzugreifen. Entweder wird ein verschlüsseltes Password an das Feldgerät gesendet, das mit Hilfe des Sicherheitsprogramms entschlüsselt und geprüft wird oder es werden die Daten die an ein Gerät gesendet werden verschlüsselt und das Sicherheitsprogramm entschlüsselt diese mit dem abgespeicherten Schlüssel.

Um eine noch höhere Sicherheit zu erhalten, wird der Sicherheitsschlüssel regelmäßig geändert. Dies kann z. B. täglich oder stündlich erfolgen. Je kürzer die Abstände zwischen dem Erzeugen eines neuen Sicherheitsschlüssels und entsprechendem Abspeichern ist, desto schwerer werden unerwünschte Manipulationen.

Vorteilhaft ist die Speicherung des Sicherheitsschlüssels nur im Feldgerät. Unter Feldgeräten sollen nicht nur Aktoren und Sensoren verstanden werden, sondern auch Controller, PLCs und Linking Devices. Im Prinzip alle Geräte, die über den Datenbus angesprochen und deren Einstellungen über den Datenbus geändert werden können.

**Patentansprüche:**

1. Verfahren zum Schutz vor unerlaubtem Zugriff auf ein Feldgerät, das über einen Datenbus mit einer Steuereinheit verbunden ist, dadurch gekennzeichnet, dass im Feldgerät ein Sicherheitsprogramm abgespeichert ist, das bei einem Zugriff auf das Feldgerät über den Datenbus eine Berechtigungsprüfung durchführt.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Sicherheitsprogramm Teil eines Funktionsblocks ist.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Sicherheitsprogramm Teil der im Feldgerät abgespeicherten Firmware ist
4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Sicherheitsprogramm einen Sicherheitsschlüssel umfasst, der bei der Konfiguration des Feldgerätes im Feldgerät abgespeichert wird.
5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Sicherheitsschlüssel zumindest ein 128 Bit-Code ist.
6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Sicherheitsschlüssel bei der Installation des Feldgerätes erzeugt wird.
7. Verfahren nach einem der vorhergehenden Ansprüche 1-5, dadurch gekennzeichnet, dass der Sicherheitsschlüssel vom Feldgerät geliefert wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Sicherheitsschlüssel regelmäßig erneuert wird.
9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Sicherheitsschlüssel stündlich erneuert wird.
10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Sicherheitsschlüssel nur im Feldgerät abgespeichert wird.
11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass Feldgeräte Sensoren, Aktoren, Controller, PLCs, oder Gateways sind.

### **Zusammenfassung**

Bei einem Verfahren zum Schutz vor unerlaubtem Zugriff auf ein Feldgerät, das über einen Datenbus mit einer Steuereinheit verbunden ist, wird im Feldgerät ein Sicherheitsprogramm abgespeichert ist, das bei einem Zugriff auf das Feldgerät über den Datenbus eine Berechtigungsprüfung durchführt.

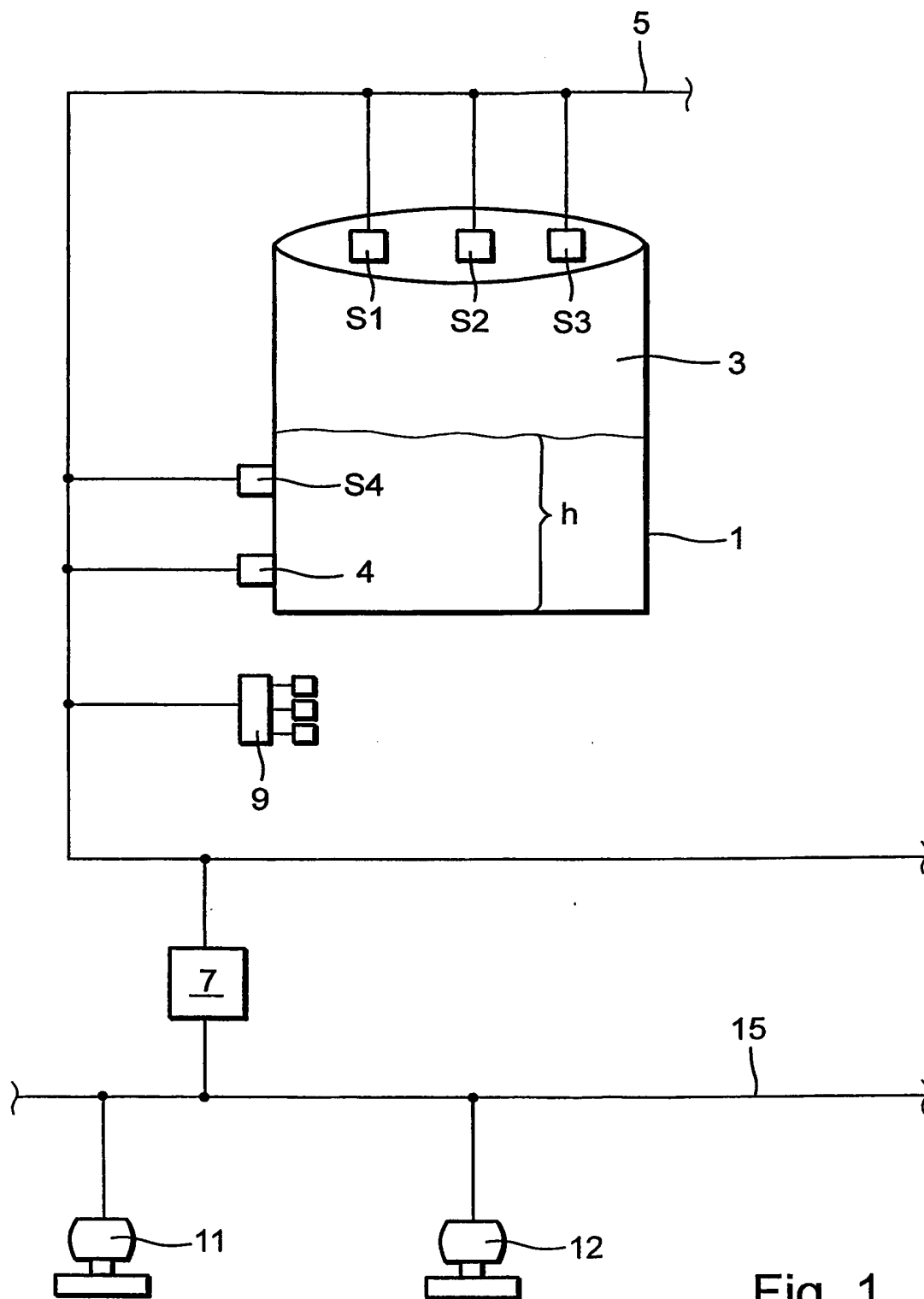


Fig. 1

212

